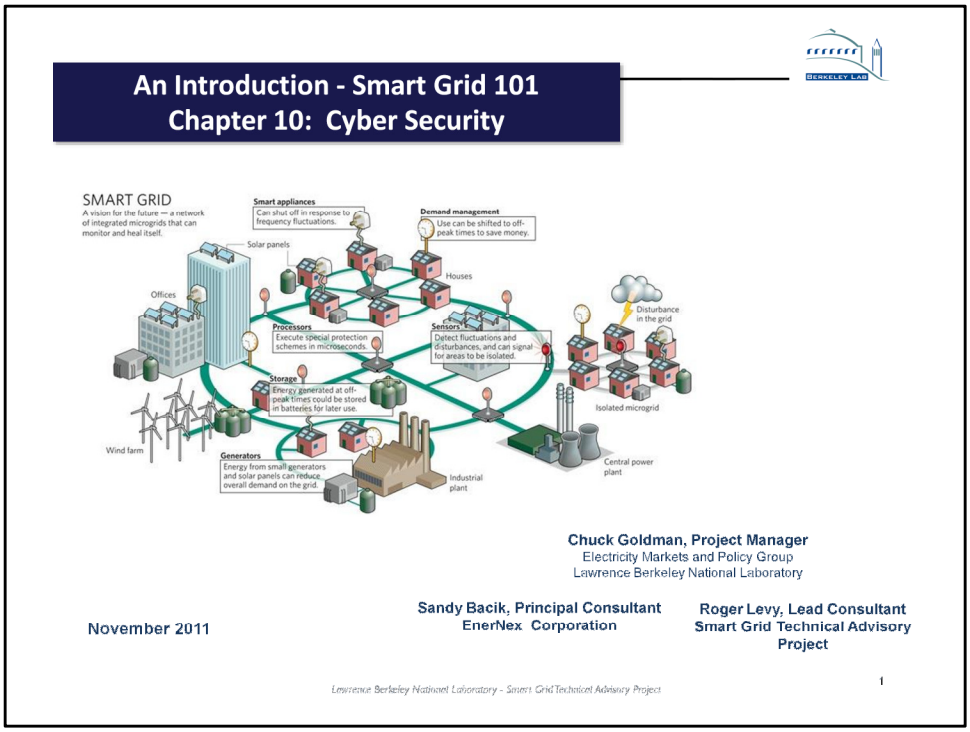
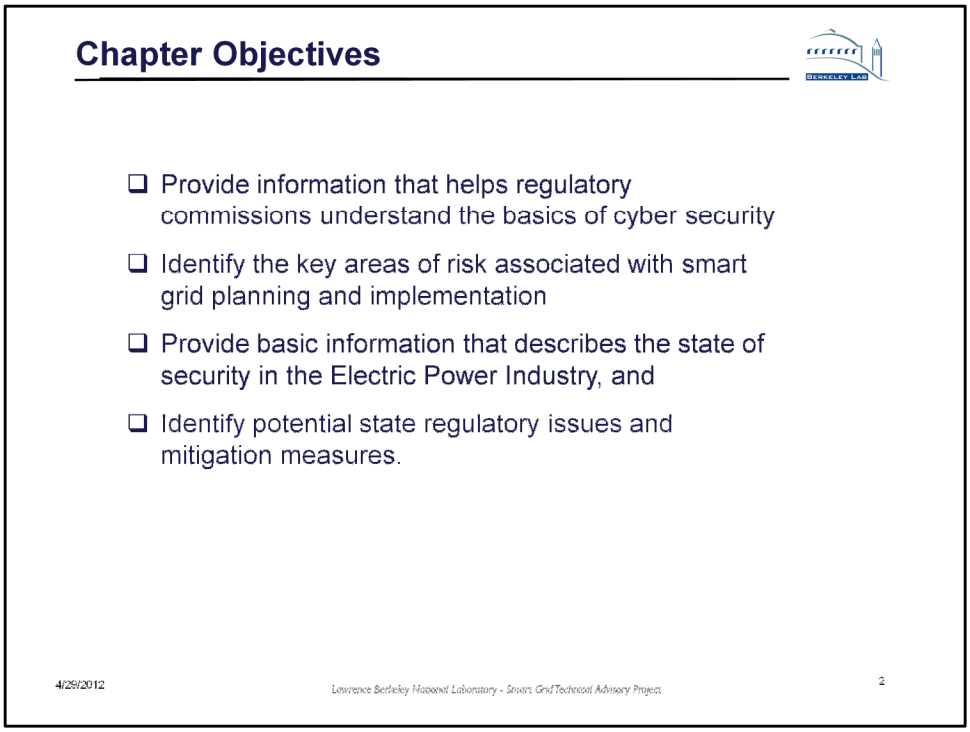


This chapter provides an overview of cyber security issues and activities by state and federal organizations Cyber security is an ongoing, high priority, active initiative within the utility industry. The activities, rules, standards, and best practices are continually being updated. As a result, the material in this presentation deck should be viewed as a starting point and initial reference guide, not a definitive statement on cyber security.

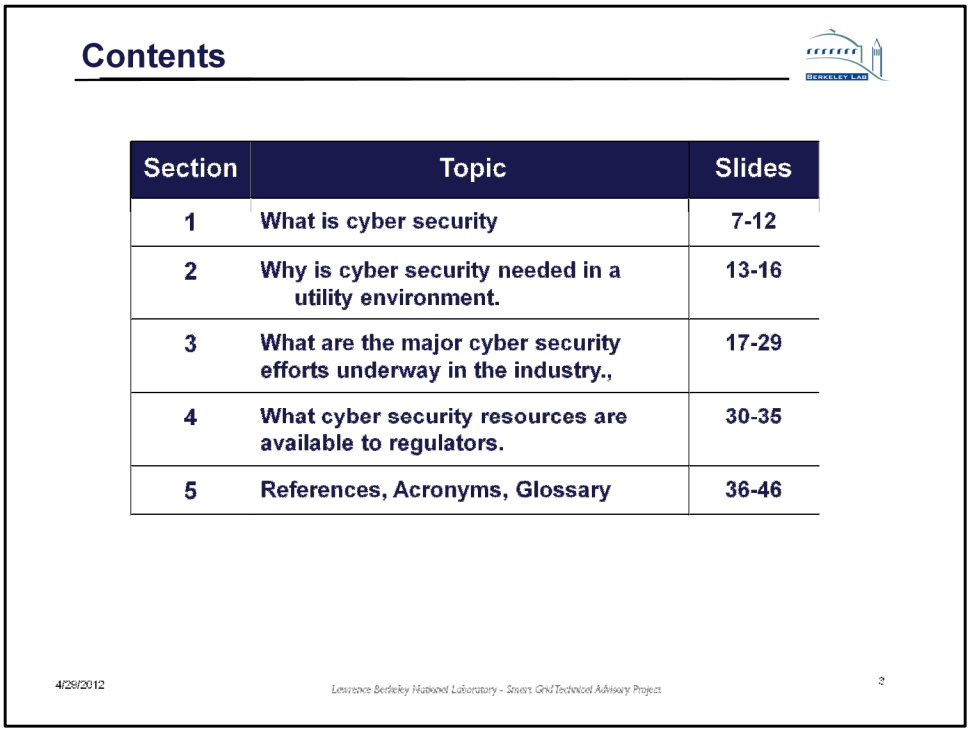
While utilities, regulators, and federal officials have always had to address physical breaches of security and sabotage, smart grid increases the opportunities for destructive or compromising incidents. The foundation of smart grid is based on the collection and communication of information that can link and integrate utility as well as customer actions into a more efficient, responsive system. Unfortunately, expanded use of monitoring, data collection and information exchanges over communication networks opens the smart grid to a world of new cyber security opportunities.

This chapter will provide an overview of the smart grid cyber security environment and the practices, standards, and other activities underway to address these threats.



This chapter has four objectives:

1. Provide information that helps regulatory commissions understand the basics of cyber security
2. Identify the key areas of risk associated with smart grid planning and implementation
3. Provide basic information that describes the state of security in the Electric Power Industry, and
4. Identify potential state regulatory issues and mitigation measures.



The contents of this chapter are divided into five sections.

References and links to organizations, articles, reports, and other resources are provided on each slide throughout this chapter. The final section provides links to supplemental reference material, a list of common cyber security acronyms, and a glossary of terminology.

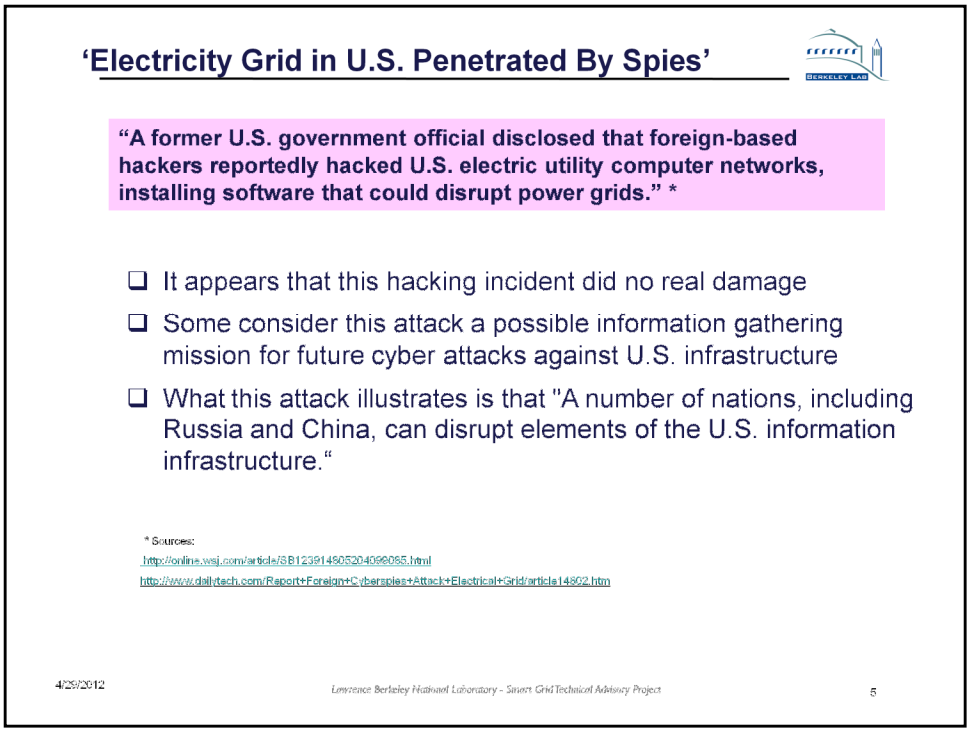
‘Slammer Worm Crashed Ohio Nuke Plant Network’

“The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant in January and disabled a safety monitoring system for nearly five hours, despite a belief by plant personnel that the network was protected by a firewall,….” *

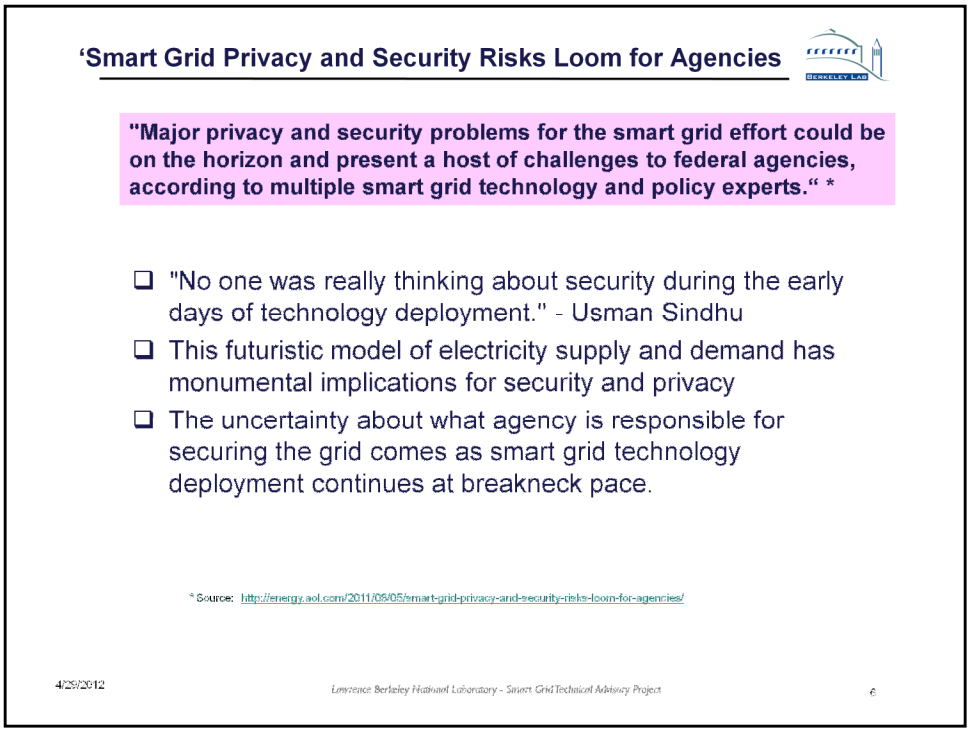
- Problem attributed to oversight in interconnection between plant and corporate network
- Breach through unsecured network of utility contractor
- Network security bypassed

* Sources:
http://www.securityfocus.com/news/6767
http://www.tofinosecurity.com/why/Case-Profile-Davis-Besse-Nuclear-Power-Plant

This slide summarizes key points from an article describing what is considered a significant cyber security attack on the Ohio Davis-Besse Nuclear Power Plant. The fact that this attack was successful, means that it could be replicated with more severe consequences at other nuclear plants in the U.S. and elsewhere. What is also interesting is that the avenue of attack was not through a utility system but through a network of a utility contractor. What this SLIDE illustrates is that cyber security must address every internal and external utility touch-point.

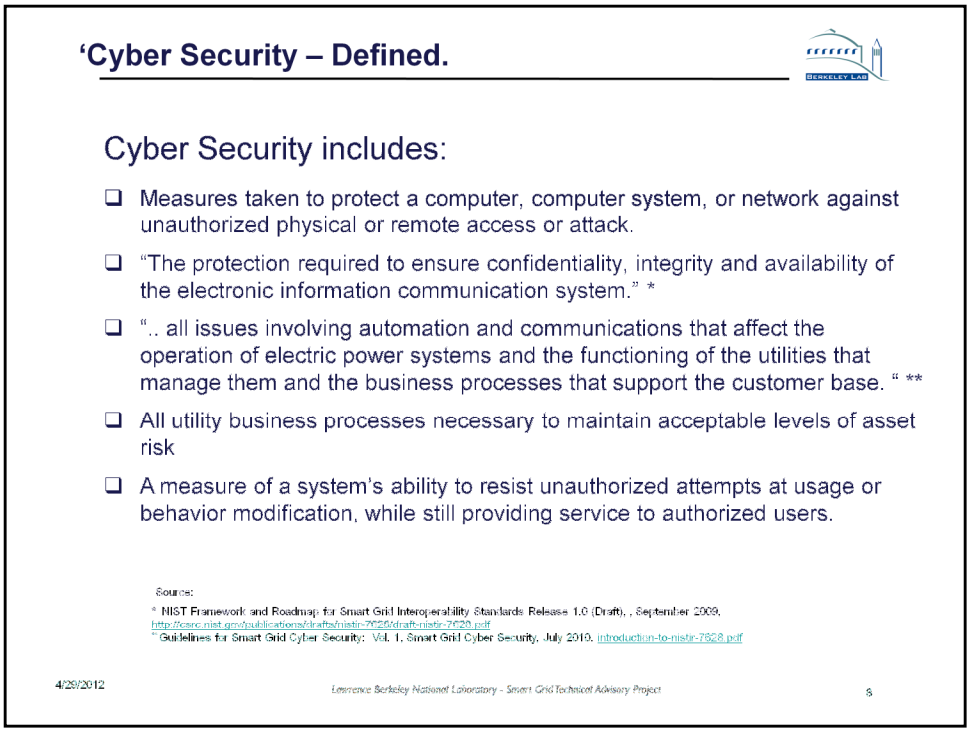


This example provides another illustration of the active environment and international nature of cyber security activity. These attributes alone make local regulation and oversight especially difficult.



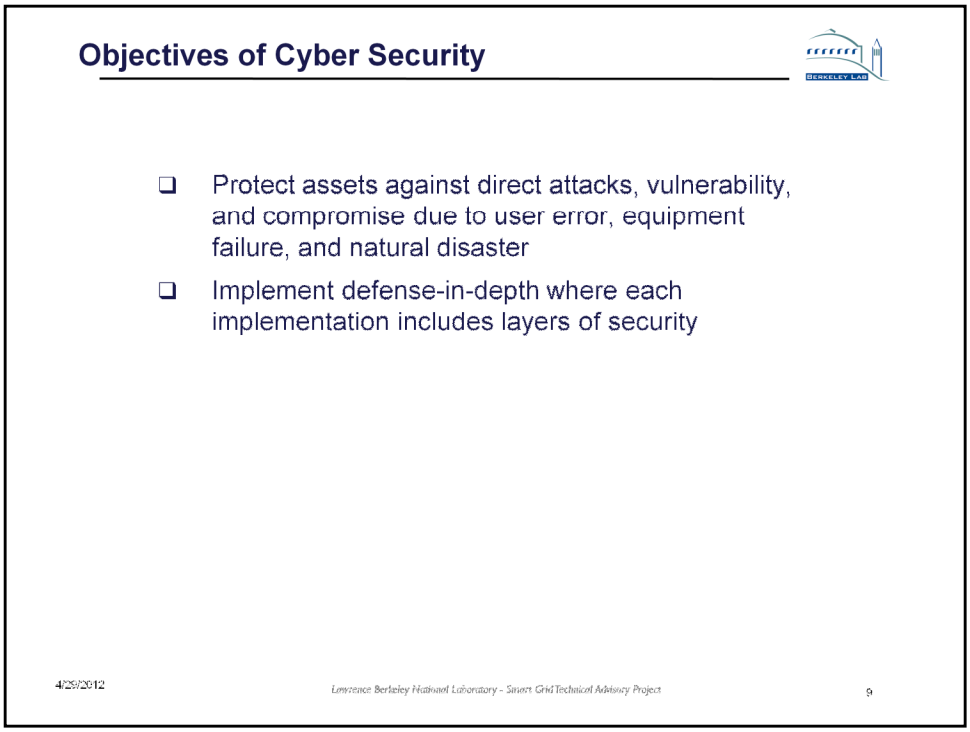
Cyber security may not be a new threat, but with increased emphasis on communications technology that impacts the electricity supply and delivery system, utilities and local regulatory authorities must prepare for more challenges in the future.

What is Cyber Security?



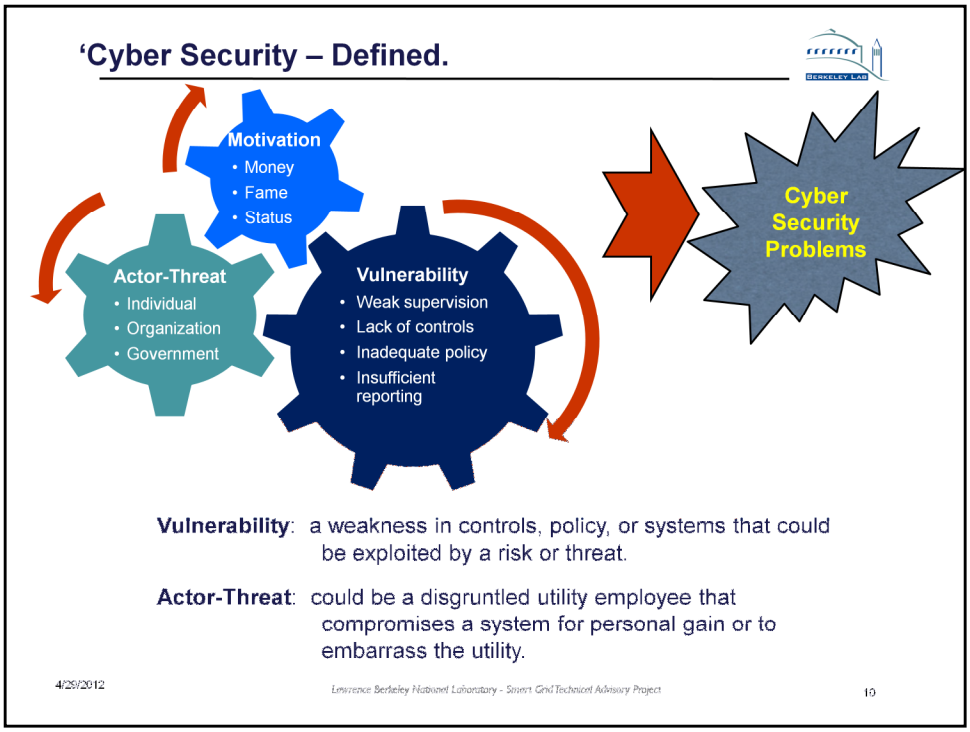
Under a smart grid environment, the electric sector will become increasingly dependent on information technology (IT). Contrary to some perspectives, the information infrastructure includes more than just computers, terminals and communication systems. IT includes hardware, software, and firmware common to IT systems, however it also includes the processes, industrial control systems (ICS) and people, and all physical systems and facilities necessary to process, store, and transmit information within a utility and between a utility, its customers and all business partners.

Security requirements also include the management, operational, and technical safeguards or countermeasures prescribed for IT and industrial control systems (ICS). Understanding the overall effectiveness of the security requirements implemented in the system and its environment of operation is essential in determining the risk to the organization's operations.



Attacks against assets can be physical, logical, and even social (e.g., talking your way into a control center). Assets need to be protected using what is referred to as a 'defense-in-depth architecture', meaning a bad person or insider would have to compromise many systems or items to corrupt an asset. Using depth in defense is a key cyber security objective in protecting an asset. A specific example of depth in defense would be as follows:

- Layer 1, Using perimeter security, such as facility access badges
- Layer 2, Using device security, such as an account and password
- Layer 3, Using application security, such as using role-based security
- Layer 4, Using database security, such as using additional configuration controls for accounts, roles, and specific transactions



Cyber security is typically defined as the collective use of standards, practices, rules, and processes to protect an organization and its assets from internal and external vulnerabilities and threats.

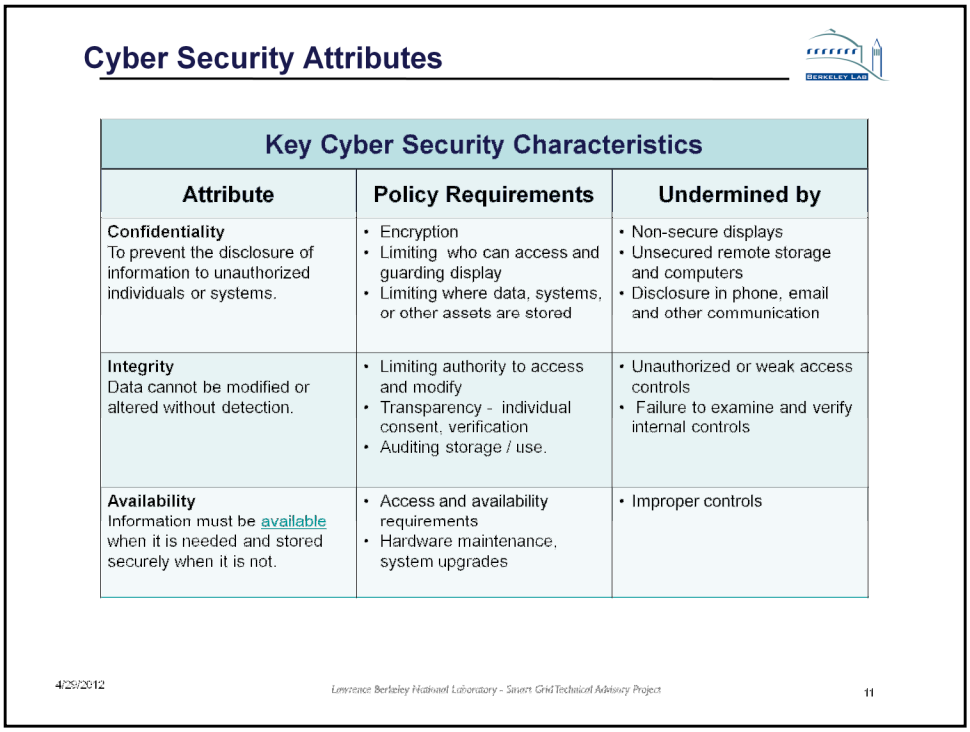
Assets can include physical building, equipment and systems as well as the integrity of communication links, data, and business relationships.

An asset can be exploited by any incident that jeopardizes its original purpose or operation. Threat s raise the risk for a potential loss.

The motivation behind a cyber security breach can be something as simple as a disgruntled employee or customer seeking to obtain free electricity. Any motivation could cause a cyber security weakness, if the action taken to accomplish the motivation is to destroy, corrupt, or modify an asset.

A few examples of cyber security weaknesses include

- Hackers / crackers – external unauthorized individuals or organizations attempting to gain access to systems
- Disgruntled / inexperienced employees –who do not receive proper training to perform their job and inadvertently compromise a system or database or allow unauthorized access to those systems and databases
- Competitors, partners, third parties – external entities that want to take advantage of a utility or seek retribution for a failed contract or relationship



Cyber Security Attributes

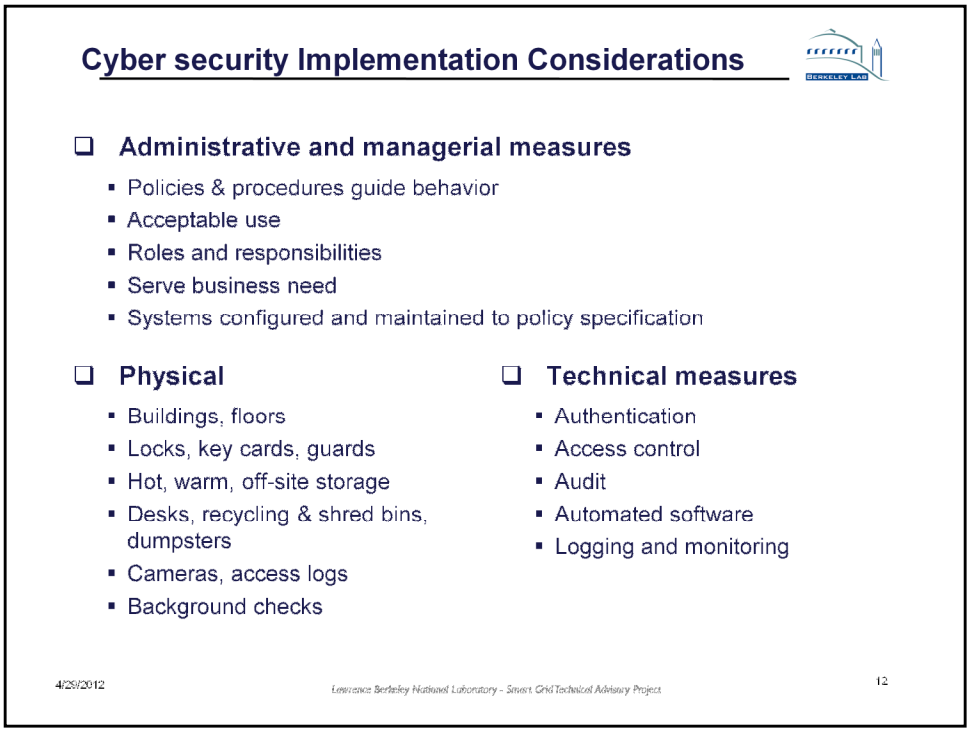
Key Cyber Security Characteristics

Attribute	Policy Requirements	Undermined by
Confidentiality To prevent the disclosure of information to unauthorized individuals or systems.	• Encryption • Limiting who can access and guarding display • Limiting where data, systems, or other assets are stored	• Non-secure displays • Unsecured remote storage and computers • Disclosure in phone, email and other communication
Integrity Data cannot be modified or altered without detection.	• Limiting authority to access and modify • Transparency - individual consent, verification • Auditing storage / use.	• Unauthorized or weak access controls • Failure to examine and verify internal controls
Availability Information must be available when it is needed and stored securely when it is not.	• Access and availability requirements • Hardware maintenance, system upgrades	• Improper controls

Cyber security is characterized by three key attributes: confidentiality, integrity and availability.

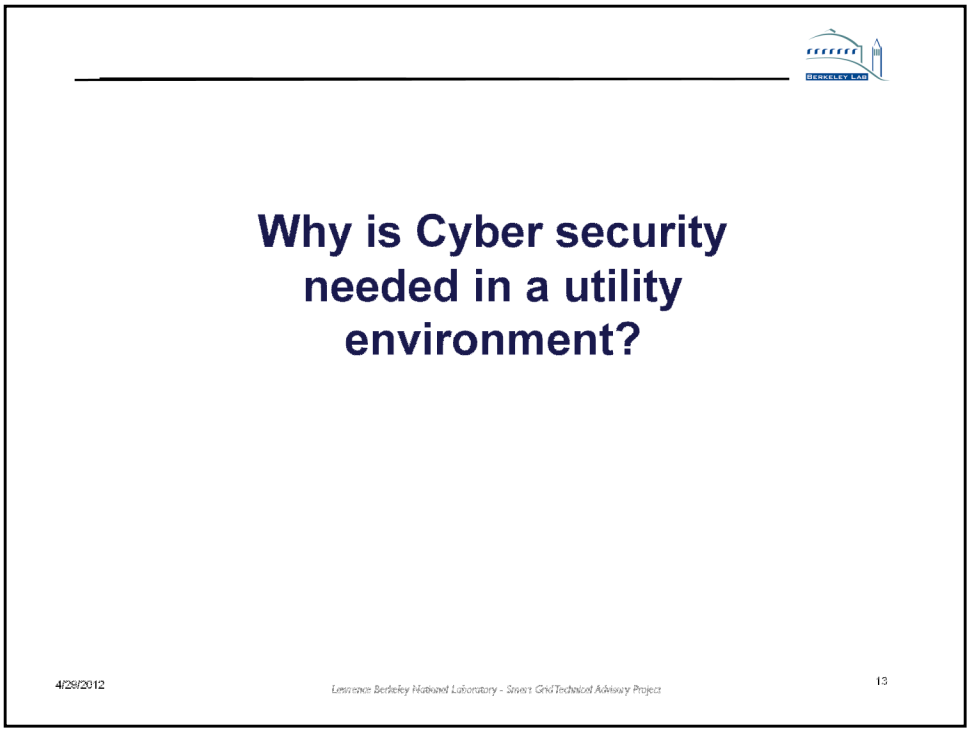
- Confidentiality refers to the limits placed on who can get access to information and what types of information they are allowed to obtain.
- Integrity refers to two related attributes: (1) the measures used to assure information is correct, and (2) that the processes used to collect and maintain information are not compromised in such a way as to violate the first attribute.

  Any unauthorized modification of data, whether deliberate or accidental, is a breach of data integrity. Integrity can require procedures that assure information is validated and checked before being stored on a system.
- Availability describes how a system or information is stored and accessed. Where and how information is stored directly determines whether confidentiality and integrity can be maintained. How information is accessed and how original and processed information is stored and backed up are also critical.

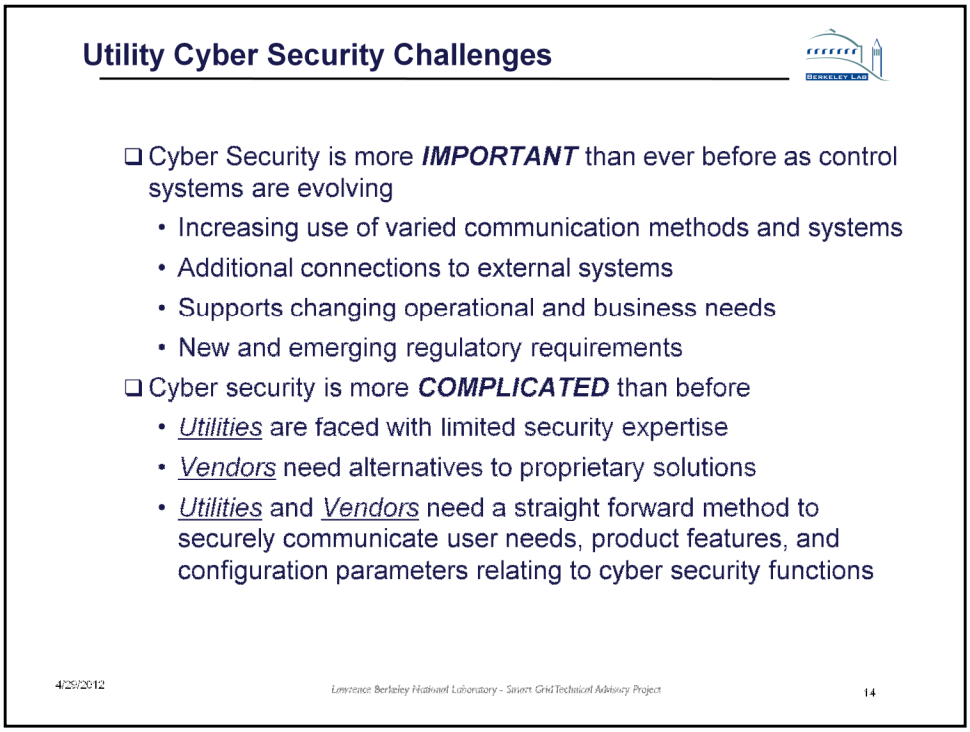


The characteristics or attributes of cyber security are very dependent upon the administrative measures, processes, and physical environment in which systems and data are implemented and maintained.

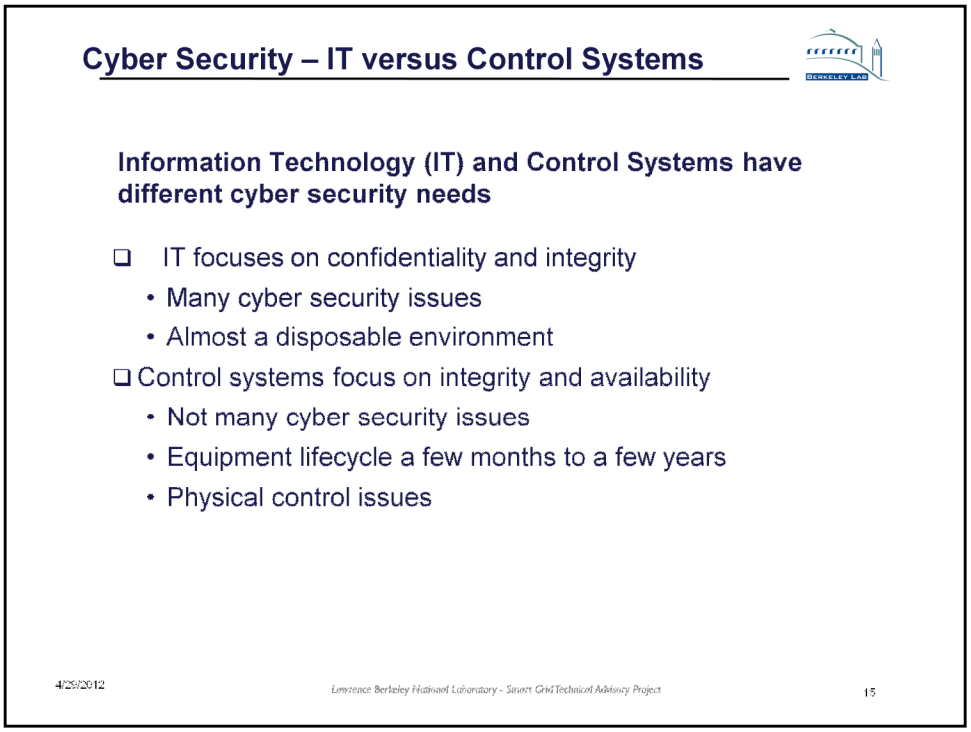
Administrative or managerial measures include policies, guidelines, standards, and processes that address who should be doing what, where, why, and how to protect an asset. Based on the administrative or managerial measures and other business requirements, the utility will then implement actual technical and physical measures to protect those assets.



Utilities have fiduciary and legal responsibilities to deliver energy reliably, safely, and within authorized contractual and regulatory approvals. Cyber security breaches can jeopardize actual system operation, the safety of the electric system, utility employees, the public and individual customers. Unauthorized access to customer data, billing records, and other business systems can incur potential civil and legal liabilities.

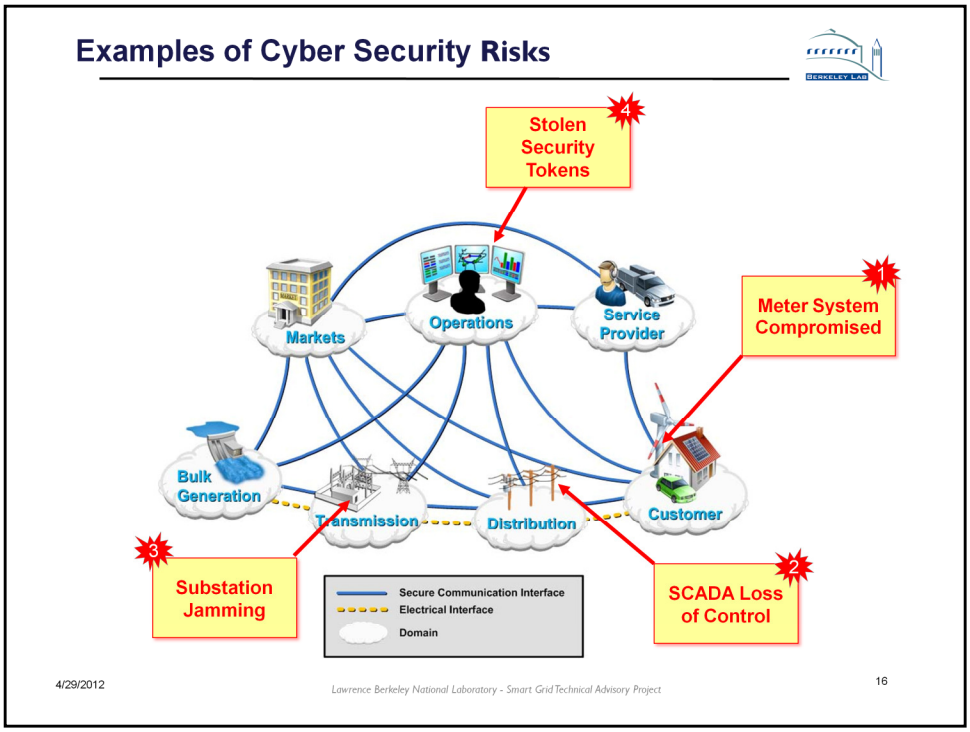


Cyber security always works best under an environment that is stable, with processes governed by universal standards, and few participants. Unfortunately, smart grid is characterized by a completely different environment - lack of stability due to the evolving nature of the systems, technology, standards, and regulations, as well as an expanded level of participation that now includes the customer and a wide variety of third-party service providers on both the utility and customer side of the meter. Furthermore, the information and communication infrastructure of smart grid opens up entirely new opportunities for cyber security problems.



Another key issue that many utilities and regulators are facing is a merging of the control system infrastructure and the corporate IT (Information Technology) infrastructure. In the past, control systems were completely separate from the corporate IT environment. With the need to integrate systems and process under smart grid, these two infrastructures which use to operate independently are now being linked to interoperate and exchange information more frequently. The cyber security requirements within each infrastructure are different and many IT requirements and controls cannot be implemented within a control system environment. Even the focus of the cyber security attributes are different within an IT and control system infrastructure.

So there is a great need for a utility to have a formalized cyber security and risk management program developed, implemented, reviewed and tested, and updated based on reviews and test results.



A regulator only has to look at the utility environment as it extends from generation to distribution system to the consumer, to observe a number of potential cyber security risks and threats that present themselves in different ways in different situations. A few examples:

1. Within the Customer domain, an attacker compromises a meter on a consumers home that uses medical equipment. The attacker performs an unauthorized remote disconnect and one of the residents dies due to lack of power to the medical equipment.

   While this is an extreme example, consider a recent news article highlighting a much less sophisticated cyber security breach in Puerto Rico.* In this case the FBI investigation indicates that former employees obtained access to optical port readers , accessed customer meters and modified internal settings to record reduced usage levels. This hacking took place on regular meters, not smart meters with communication links. Lack of proper internal security over uninstalled meters, meter software, and other field service devices can create cyber security issues. While it is speculated that the Puerto Utility may have suffered hundreds of millions of dollars in losses, some meter engineers suggest that the problem could have been identified early on with proper monitoring in the utility meter data management system. So cyber security problems and solutions don't have to be high-tech.

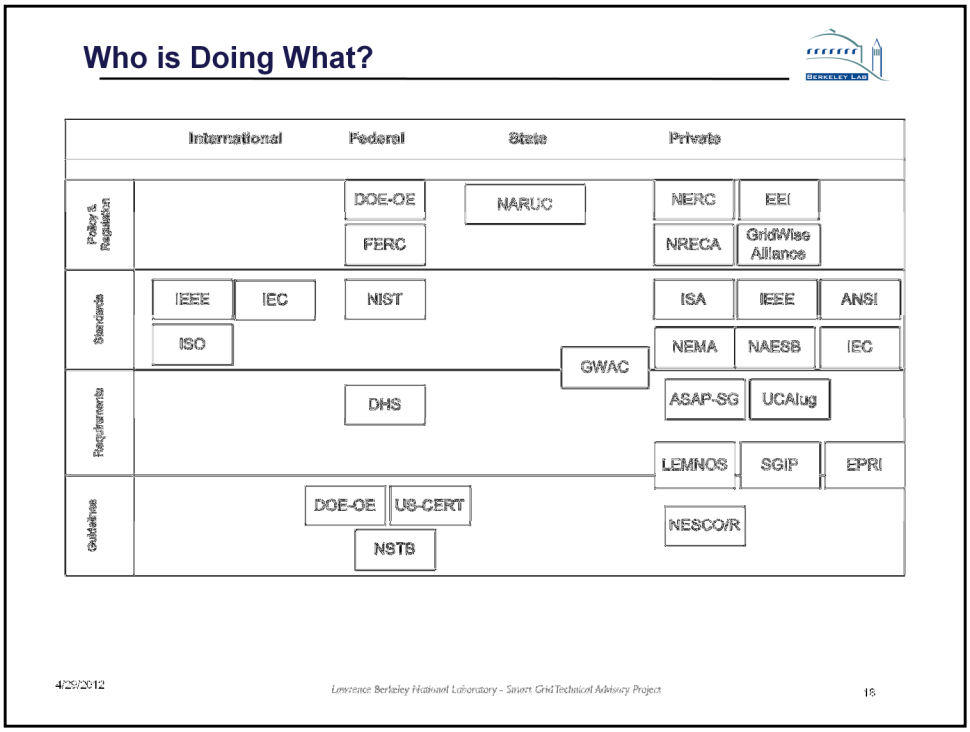
2. For secure remote access, a utility might use a token method for gaining entry to a secure environment. There is a potential that the RSA Secured tokens could be stolen, then millions of tokens could be e-issued resulting in large operational impact and system vulnerability.

3. Within the Transmission domain, a utility uses a wireless technology for communication. What would happen if wireless jamming techniques were used to stop operational processing of commands within a substation?

4. Within the Distribution domain, if the availability or recovery of a SCADA (supervisory control and data acquisition) was impeded or slowed down when being implemented, how much loss of operational functionality would happen.

* http://www.infosecisland.com/blogview/20971-FBI-Increasingly-Concerned-About-Smart-Meter-Hacks.html

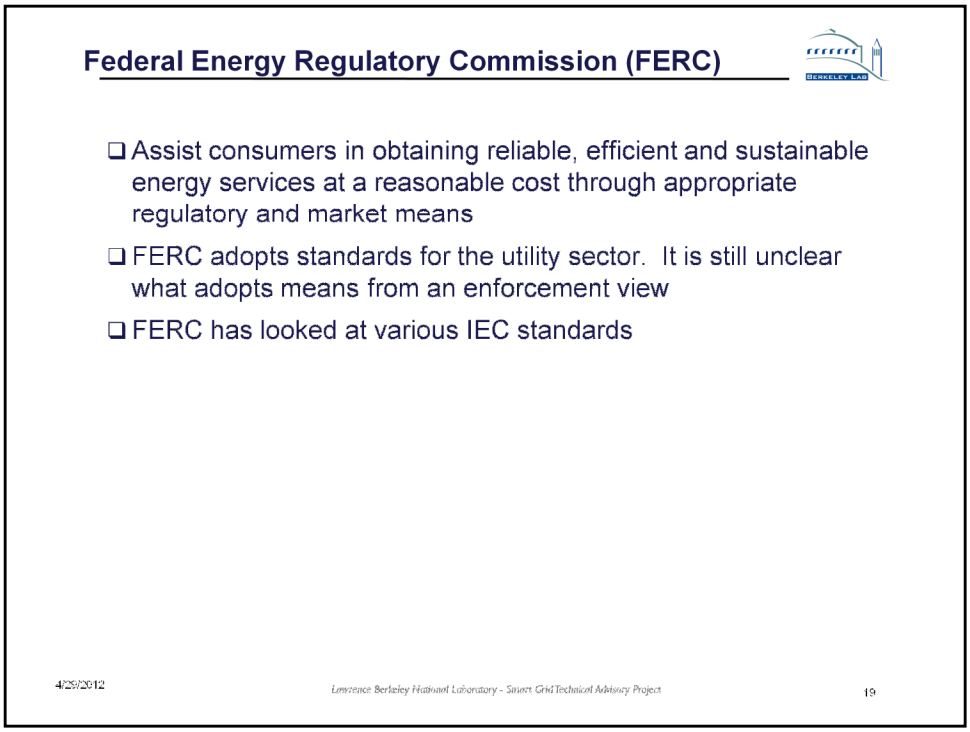
How is the Utility Industry Addressing Cyber Security



The organizations listed in this slide are actively involved in Smart Grid development, but this is not an exhaustive list.

The reference section starting on Slide 36 contains a listing of all the acronyms, a short description of each organization, and where they fit into the Smart Grid.

The next few slides will highlight some organizations and key cyber security developments to watch within the Smart Grid.

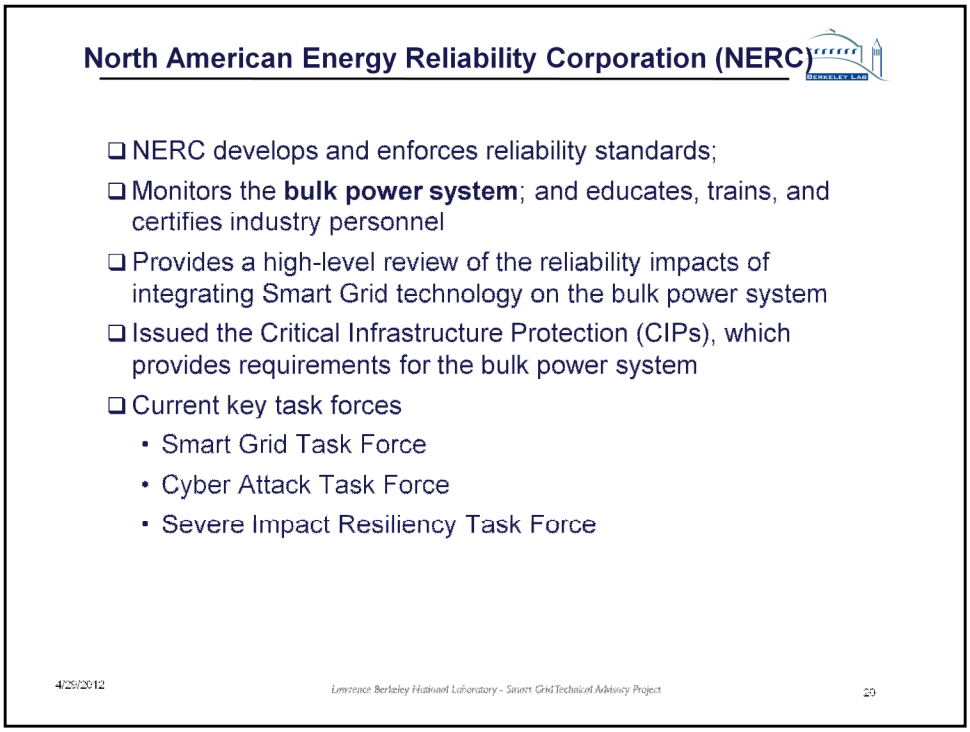


"The Energy Policy Act of 2005 (Energy Policy Act) gave the Federal Energy Regulatory Commission (Commission or FERC) authority to oversee the reliability of the bulk power system, commonly referred to as the bulk electric system or the power grid. This includes authority to approve mandatory cyber security reliability standards.

The North American Electric Reliability Corporation (NERC), which FERC has certified as the nation's Electric Reliability Organization, developed Critical Infrastructure Protection (CIP) cyber security reliability standards. On January 18, 2008, the Commission issued Order No. 706, the Final Rule approving the CIP reliability standards, while concurrently directing NERC to develop significant modifications addressing specific concerns.

Additionally, the electric industry is incorporating information technology (IT) systems into its operations – commonly referred to as smart grid – as part of nationwide efforts to improve reliability and efficiency. There is concern that if these efforts are not implemented securely, the electric grid could become more vulnerable to attacks and loss of service. To address this concern, the Energy Independence and Security Act of 2007 (EISA) gave FERC and the National Institute of Standards and Technology (NIST) responsibilities related to coordinating the development and adoption of smart grid guidelines and standards."*

* http://www.ferc.gov/industries/electric/indus-act/reliability/cybersecurity.asp



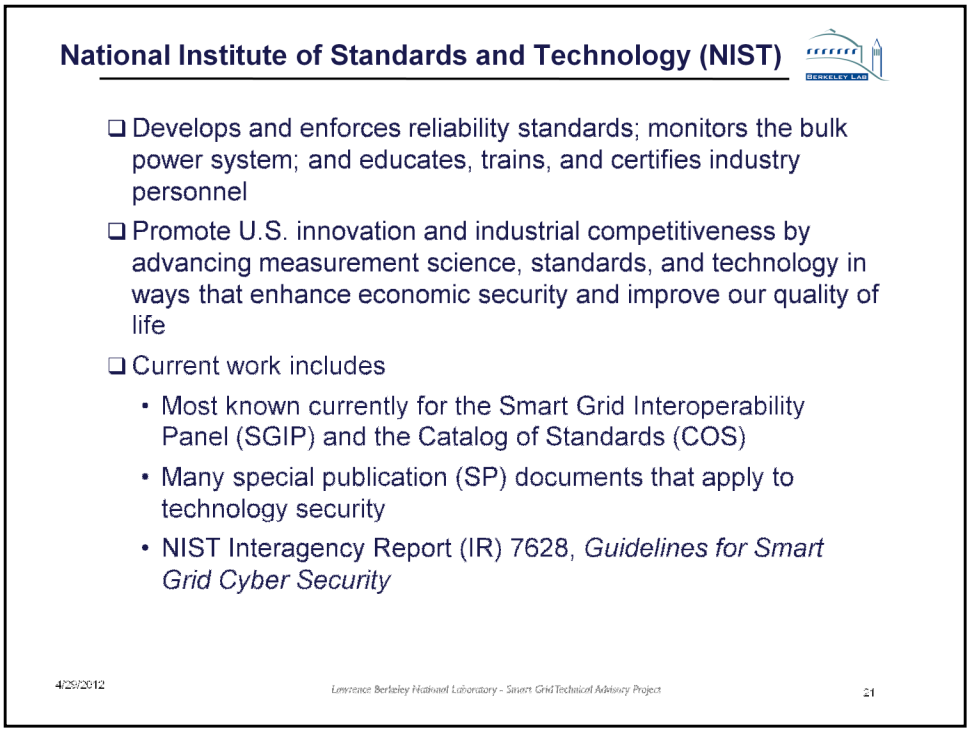
"The North American Electric Reliability Corporation's (NERC) mission is to ensure the reliability of the North American bulk power system. NERC is the electric reliability organization (ERO) certified by the Federal Energy Regulatory Commission to establish and enforce reliability standards for the bulk-power system. NERC develops and enforces reliability standards; " *

NERC has approved a substantial number of standards**, however not all of these standards have been approved by governmental authorities – which renders them unenforceable.

NERC is focused on the bulk power systems portion of the utility grid. At this time, NERC continues to update and maintain the Critical Infrastructure Protection (CIP) requirements. NERC is also in the process of giving guidance to utilities on implementing the CIPs and additional requirements in protecting utility assets. In November 2011, NERC completed their first cyber security exercise with bulk utilities.

* http://www.nerc.com/

** http://www.nerc.com/page.php?cid=2%7C20



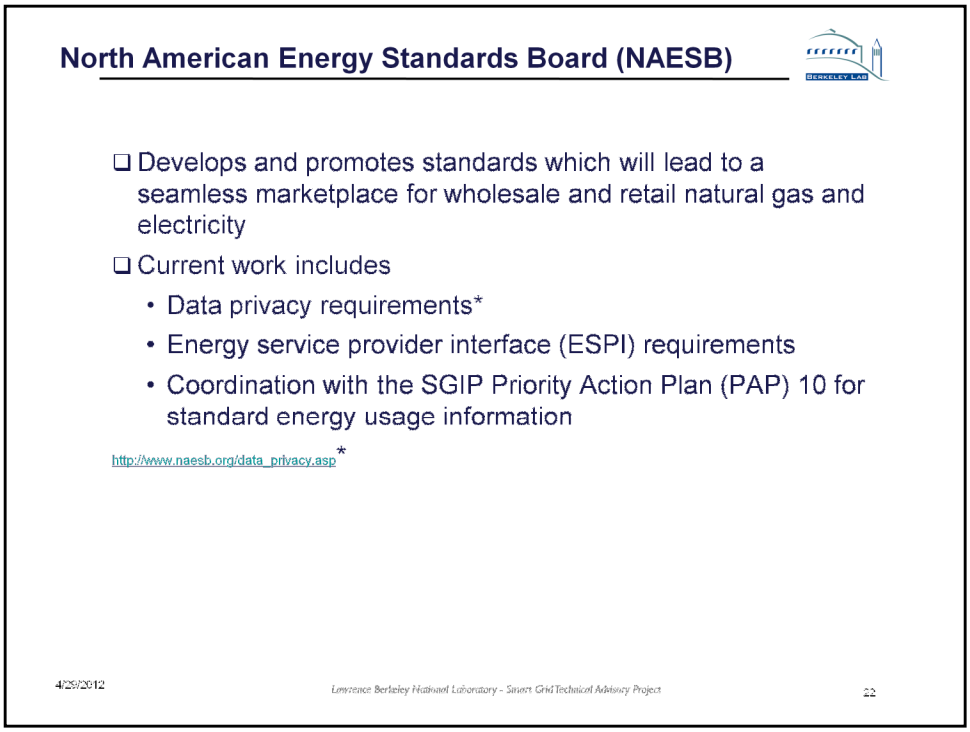
The SGIP (http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/WebHome) has been built on NIST funding to coordinate standards development for the Smart Grid.

The SGIP CoS based on the *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0* (NIST SP 1108) (Office of the National Coordinator for Smart Grid Interoperability, National Institute of Standards and Technology, *NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 1.0 (NIST SP 1108)*, Jan. 2010. The report can be downloaded at: http://nist.gov/smartgrid/) standards list and had been expanded to contain the SGIP Priority Action Plan (PAP) standards and guidelines. The CoS is a listing of standards that have been reviewed by the SGIP and the SGIP votes as to whether the standards is applicable to the Smart Grid.

Currently, the NIST Interagency Report (IR) 7628, Guidelines for Smart Grid Cyber security is the most notable source for cyber security requirements within the smart grid. While this source is not normative, some utilities are making this document a requirement.

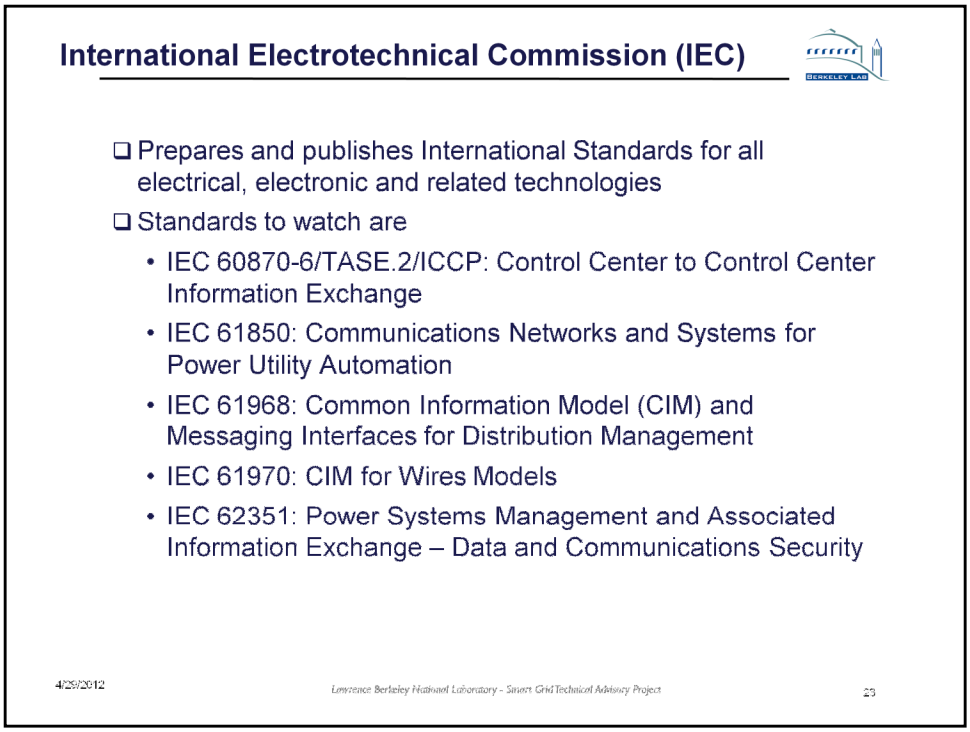
Reference

1. Introduction to the NISTIR 7628: http://www.smartgrid.gov/sites/default/files/pdfs/nistir_7628%20.pdf
2. NISTIR 7628 Volume 1: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol1.pdf
3. NISTIR 7628 Volume 2: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol2.pdf
4. NISTIR 7628 Volume 3: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf



The NAESB Board has created the Critical Infrastructure Committee (CIC) whose task is to collect and report information related to cyber security threats, legislation, and industry cyber security activity. The efforts of the NAESB CIC can be monitored on NAESB's website at:
http://www.naesb.org/board_critical_infrastructure.asp

NAESB is currently in the process of focusing on privacy of information. Depending upon the state and commission regulations, what NAESB develops may be in conflict to what a state may accept as their requirements. *Regulators are urged to follow this activity closely. **

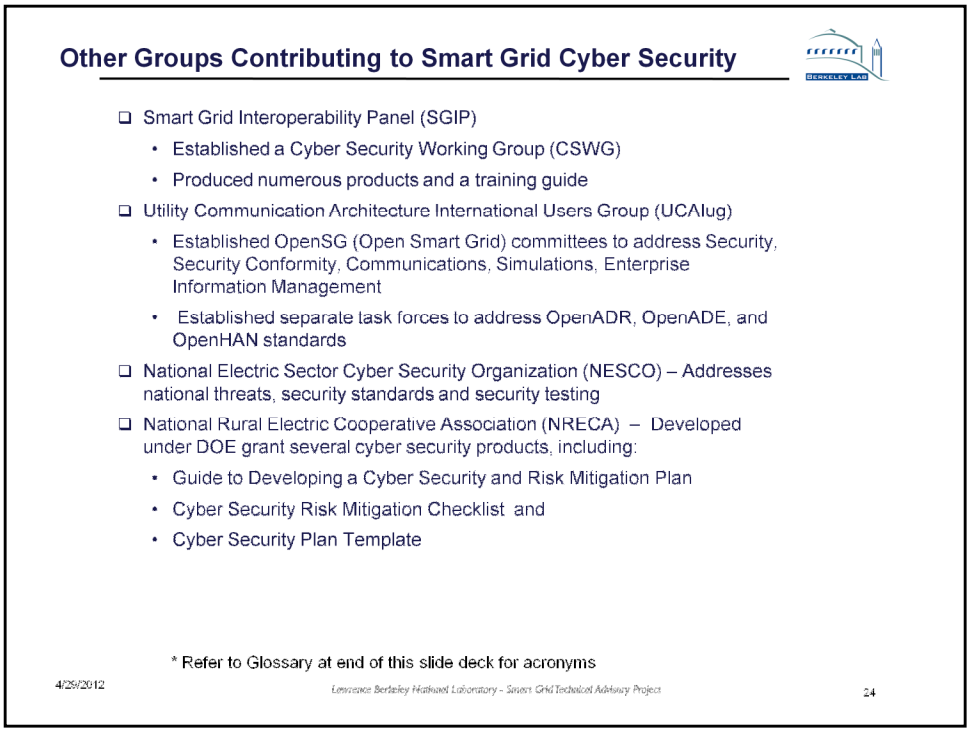


"Founded in 1906, the IEC (International Electrotechnical Commission) is the world's leading organization for the preparation and publication of International Standards for all electrical, electronic and related technologies. These are known collectively as "electro technology". IEC provides a platform to companies, industries and governments for meeting, discussing and developing the International Standards they require."

IEC 60320 is a set of standards from the International Electrotechnical Commission specifying non-locking electrical power couplers for the connection of power supply cords to electrical appliance up to 250 V.[1] Couplers described under these standards have standardized current and temperature ratings. Use of standard inlets and country-specific cord sets allows manufacturers to produce the same appliance for many markets, where only the cord set has to be changed for a particular market. Compatible connectors are also made for equipment that requires power outlets for interconnection.

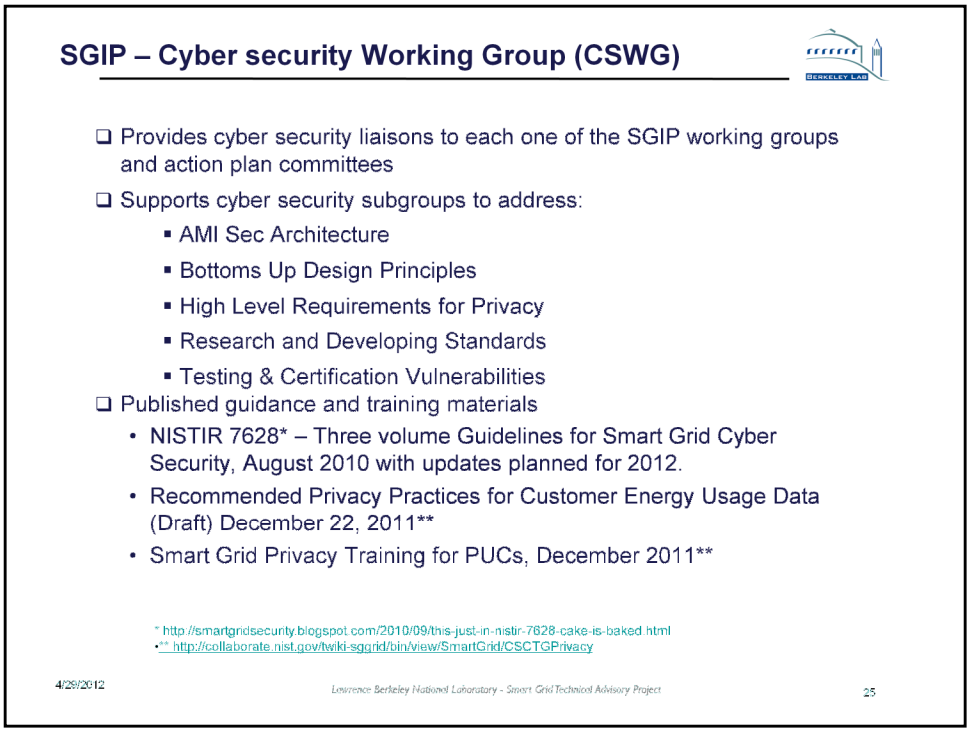
IEC continues to update their standards to include cyber security requirements. IEC, along with many standards development organizations, has a long process for developing and updating standards. The risk with the standards development organizations is by the time they issue new cyber security requirements in their standards, newer threats have come into existence and the standard and requirements may be obsolete.

* http://www.iec.ch/about/



The organizations are working on cyber security standards also. The CSWG, NRECA, and NESCO/NESCOR do not have any membership fees and are open for regulators to join.

The UCAIug does have an annual membership fee and is open for regulators to join.



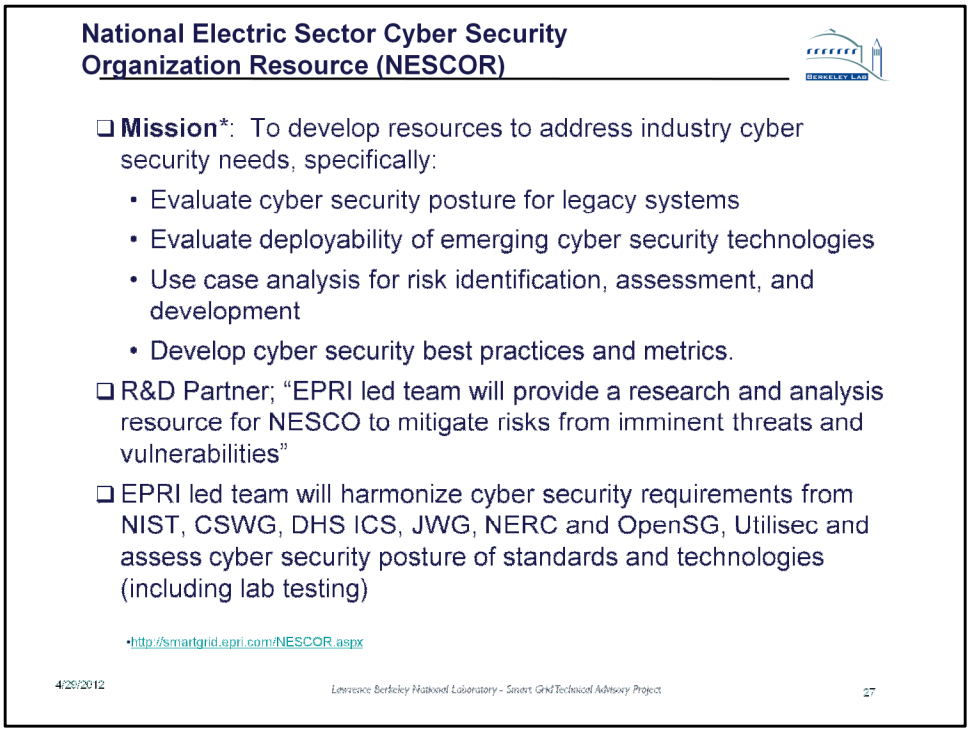
The SGIP CSWG is focused on security guidance in all Smart Grid domains. There are over 650 CSWG volunteer participants from utilities, commission, academia, laboratories, government entities, and vendors. You can learn more about each of the CSWG subgroup through the CSWG's main wiki page: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CyberSecurityCTG. Detail information can be found in the NISTIR 7628 (see Reference #7 on Slide 37). Some of the points on topic are listed below.

NIST IR 7628 identifies high level security requirements in the following control families:

- Access Control
- Awareness and Training
- Audit and Accountability
- Security Assessment and Authorization
- Configuration Management
- Continuity of Operations
- Identification and Authentication
- Information and Document Management
- Incident Response
- Smart Grid Information System Development and Maintenance
- Media Protection
- Physical and Environmental Security
- Planning
- Security Program Management
- Personnel Security
- Risk Management and Assessment
- Smart Grid Information System and Services Acquisition
- Smart Grid Information System and Communication Protection
- Smart Grid Information System and Information Integrity

"The **National Electric Sector Cyber security Organization** (or NESCO) is the first public-private partnership of its kind in the electric sector. NESCO serves as a focal point bringing together utilities, federal agencies, regulators, researchers, and academics. This group, along with domestic and international experts, developers, and users help to focus cyber security research and development priorities, to identify and disseminate effective common practices, and organize the collection, analysis and dissemination of infrastructure vulnerabilities and threats. NESCO works to identify and support efforts to enhance cyber security of the electric infrastructure. This project is being partially funded by the Department of Energy."*

•http://www.energysec.org/nesco



"The National Electric Sector Cyber security Organization Resource (NESCOR)Is intended to strengthen the cyber security posture of the electric sector by establishing a broad-based public-private partnership with the Department of Energy (DOE) for collaboration and cooperation. NESCOR serves as a focal point to bring together domestic and international experts, developers, and users to specify and, if applicable, test security of novel technology, architectures, and applications for the electric sector. NESCOR also addresses the priorities for development of products and deliverables necessary to assist industry and government in addressing the cyber security challenges to electric sector reliability.

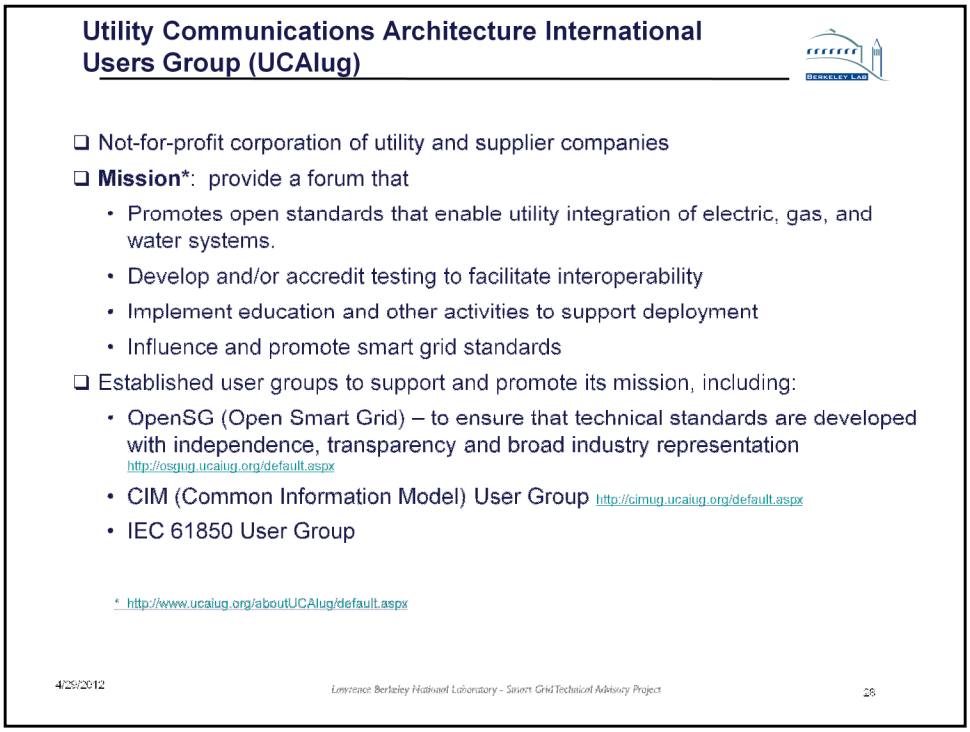
NESCOR works collaboratively with NESCO, DOE, and other federal agencies to:

- Enhance cyber security of the bulk power electric grid and electric infrastructure, including, the security of legacy, current, and emerging technologies for the electric generation, transmission, and distribution domains
- Assess security features,
- Specify security solutions and mitigation strategies,
- Focus cyber security research and development priorities, and
- Identify and disseminate best practices.

NESCOR's goal is to protect the electric grid and enhance the integration of smart grid technologies that will mitigate the effects of cyber attacks – both malicious and non-malicious. Products that are developed are intended to complement and enhance the development and implementation of key milestones and objectives called for in the Roadmap to Secure Control Systems in the Energy Sector."*

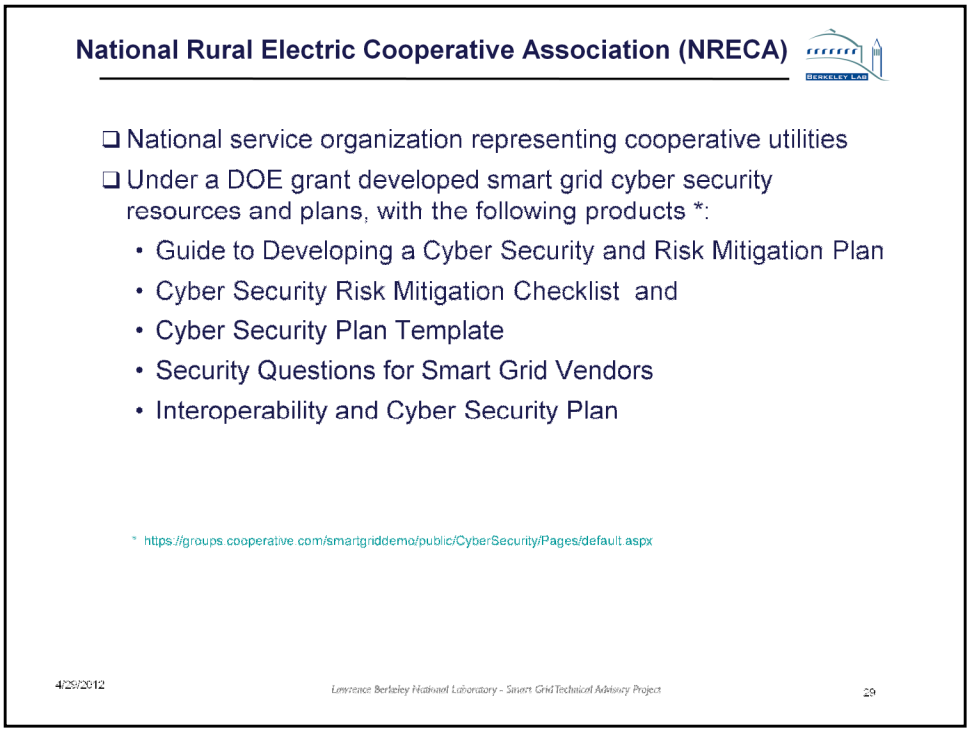
http://www.smartgrid.epri.com/NESCOR.aspx

*



"UCA International Users Group is a not-for-profit corporation focused on assisting users and vendors in the deployment of standards for real-time applications for several industries with related requirements. The Users Group does not write standards, however works closely with those bodies that have primary responsibility for the completion of standards (notably IEC TC 57: Power Systems Management and Associated Information Exchange)."*

•http://www.ucaiug.org/default.aspx



"NRECA is the national service organization for more than 900 not-for-profit rural electric cooperatives and public power districts providing retail electric service to more than 42 million consumers in 47 states and whose retail sales account for approximately 12 percent of total electricity sales in the United States."*

"The National Rural Electric Cooperative Association (NRECA) released an "Interoperability and Cyber Security Plan" (ICSP) developed by the Cooperative Research Network (CRN) for cooperatives participating in a nation-wide smart grid demonstration project. The ICSP lays out specific steps and a continuous process improvement plan for the cooperatives as well as the vendor community to meet evolving federal and industry standards. " See Reference #9 Slide #37.

* http://www.nreca.coop/ABOUT/Pages/default.aspx

.

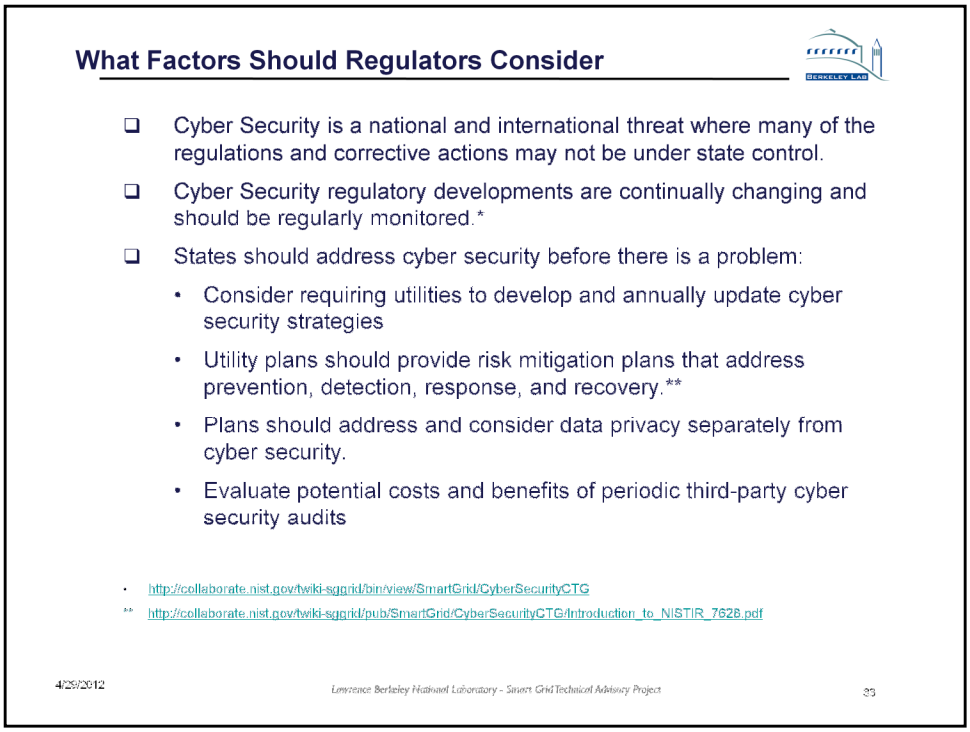
Regulatory involvement is absolutely necessary in order to insure the foundational policies around cyber security are laid before the technology is put in place.

Cyber Security Reports, Guidelines and Training Material - 1

- **SGIP Cyber Security Working Group**
  - Guidelines for Smart Grid Cyber Security http://smartgridsecurity.blogspot.com/2010/09/this-just-in-nistir-7628-cake-is-baked.html
  - Smart Grid Privacy Training for PUCs, December 2011 http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGPrivacy/CSWG_Smart_Grid_Privacy_Training_for_PUCs_December_14_2011_FINAL.pptx
- **DOE Audit Report on Smart Grid Investment Grant Cyber Security Plans, OAS-RA-12-04, January 2012** http://energy.gov/sites/prod/files/OAS-RA-12-04.pdf
- **Federal Energy Regulatory Commission's Monitoring of Power Grid Cyber Security, IG-0846** http://energy.gov/sites/prod/files/igprod/documents/IG-0846.pdf
- **NRECA Cooperative Research Network**
  https://groups.cooperative.com/smartgriddemo/public/CyberSecurity/Pages/default.aspx
  - Guide to Developing a Cyber Security and Risk Mitigation Plan
  - Cyber Security Risk Mitigation Checklist and
  - Cyber Security Plan Template
  - Security Questions for Smart Grid Vendors
  - Interoperability and Cyber Security Plan
- **SmartGrid.Gov – complete listing of reports, organizations, and working groups addressing cyber security**
  http://www.smartgrid.gov/recovery_act/overview/standards_interoperability_and_cyber_security/cyber_security

Cyber Security Reports, Guidelines and Training Material - 2

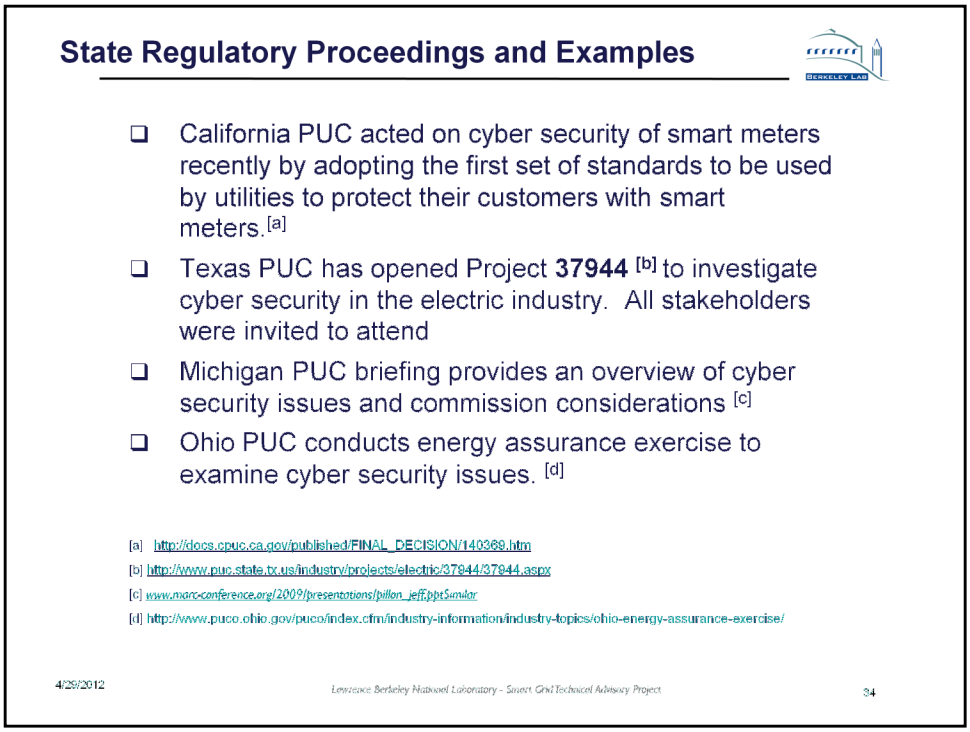
- **Electricity Sector Cyber security Risk Management Process Guideline,** U.S. Department of Energy, September 2011, https://public.commentworks.com/CW_DOE_WF/InitiativeDocFiles/46/RMP_Guideline_Draft_for_Public_Comment_08312011-1.pdf
- **Roadmap to Achieve Energy Delivery Systems Cyber security,** Energy Sector Control Systems Working Group, September 2011, http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf
- **Vulnerability Analysis of Energy Delivery Control Systems,** Idaho National Laboratory, September 2011, http://energy.gov/oe/downloads/vulnerability-analysis-energy-delivery-control-systems
- **Roadmap to Secure Energy Delivery Systems, Draft,** Energy Sector Control Systems Working Group, January 2011, http://energy.gov/sites/prod/files/Energy%20Delivery%20Systems%20Cybersecurity%20Roadmap_finalweb.pdf
- **Electricity Grid Modernization, Progress Being Made on Cyber security Guidelines, but Key Challenges Remain to be Addressed,** U.S. Government Accountability Office, GAO-11-117, January 2011, http://www.gao.gov/new.items/d11117.pdf



What can be done? When is the best time to begin taking cyber security seriously, before an event happens or afterwards? Taking action to protect the public after the harm has been inflicted is not what is generally accepted as a best practice by regulators. Now, while the smart grid is evolving is the best time to begin the process.

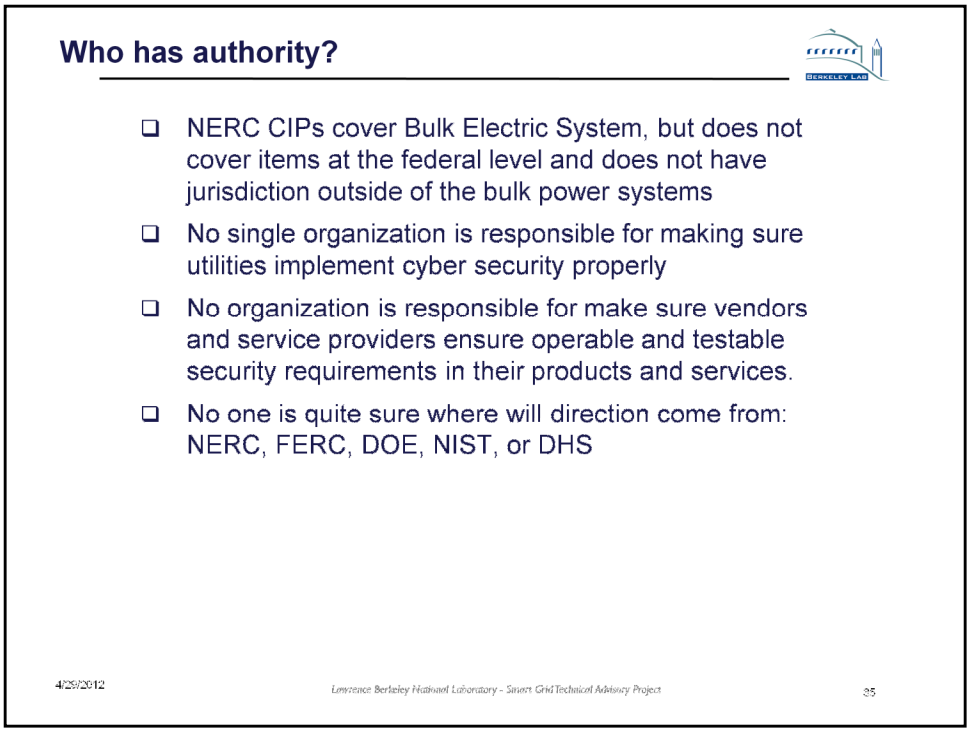
The SGIP has a working group web page containing a tremendous amount of information on cyber security and it is available to anyone (see link provided in the references). Start there.

Others are already moving forward. Some commissions are way ahead of others in dealing with this urgent issue. It may not be feasible or legal to adopt what another state has adopted carte blanche because utilities are different, state commissions are different, and laws are different generally. It is however prudent for any regulator to view what the early adopters have decided and consider the process used by that particular commission as a guide. Who is acting on cyber security right now? California recently issued a decision on cyber security (August 2011). Texas has a project on privacy and security. There are others.



The CPUC rulemaking implements protections ordered by Senate Bill 1476 which was signed into law September of 2010. It is based on Fair Information Practices, or FIPs, developed by the Department of Homeland Security. The decision places limits on the amount and kind of information that SCE, SDG&E, and PG&E can share with companies which collaborate (with the utility or with the customer) in meter installation, monitoring, data collection, renewable energy installations or energy efficiency retrofitting. Texas PUC is discussing cyber security, but as of this writing a decision or rule making proceeding has not happened.

The cyber security actions taken by the California PUC is a starting point, although it is too early to determine if these are the 'correct' or best guidelines.



The NERC CIPs were developed for the bulk electric system, yet depending on how utility assets are described and qualified, the increasing number of control points and load shed capabilities in smart meters may begin to qualify a smart meter as a critical asset and fall under the NERC CIPs.

NERC reports into FERC and FERC evaluates the work that NERC is completing, yet NERC does not have the federal authority to enforce their CIPs across all smart grid domains.

At this time, no federal level organization has a good handle on the items needed to move smart grid technology forward in a secure manner. Discussions continue at the federal level as to where the enforcement and "decreeing" of requirements and standards will go towards the whole utility sector. No federal organization is the clear front runner for taking on that responsibility.

Some state regulators are stepping up to create regulations designed to assist in helping with asset protection. One issue to consider is what happens if state cyber security regulations are developed and implemented and later, a federal regulation is implemented, and is in conflict with the implemented state cyber security regulation. Will the state regulation be repealed or amended or left to stay?

Consequently, at this time, it is suggested that state regulators 'wait and see' before passing specific cyber security reforms and rules

References

Supplemental References

	Title	Link
1	Comments of the National Cable & Telecommunications Association on NBP Public Notice #2, FCC GN Docket No. 09-47, 09-51, 09-137, November 13, 2009	http://www.google.com/#sclient=psy&hl=en&safe=off&rlz=1R2ADRA_enUS410&q=COMMENTS+OF+THE+NATIONAL+CABLE+%26+TELECOMMUNICATIONS+ASSOCIATION+ON+NBP+PUBLIC+NOTICE+%232&aq=&aqi=&aql=f&oq=&pbx=1&bav=on.2,or.r_gc.r_pw.&fp=a4cc8d06c4568ecd
2	Smart Grid White Paper, The Home Appliance Industry's Principles & Requirements for Achieving a Widely Accepted Smart Grid, AHAM, December 2009	http://www.aham.org/ht/a/GetDocumentAction/i/44191
3	Energy Management, A Mass Market Consumer Opportunity	http://ase.org/sites/default/files/BBY%20Energy%20Management%20White%20Paper.pdf
4	Get Smart, IEEE Power & Energy Magazine, May/June 2010	http://www.ieee.org/organizations/pes/public/2010/may/current.html Note: Available to IEEE members.
5	DOE ARRA Cyber Program, (2009)	https://www.arrasmartgridcyber.net/index.php
6	NERC Critical Infrastructure Protection standards, CIP 002-009	,http://www.nerc.com/page.php?ci
7	NISTIR 7628: Guidelines for Smart Grid Cyber security, August 2010,	http://csrc.nist.gov/publications/PubsNISTIRs.html#NIST-IR-762
8	Security Profile for Advanced Metering Infrastructure, Version 2.0, June 22, 2010	http://www.smartgridipedia.org/images/9/90/AMI_Security_Profile_-_v2_0.pdf
9	•Interoperability and Cyber Security Plan: NRECA Smart Grid Demonstration Project •A Pragmatic Approach to Security the Grid: Key Points	http://www.nreca.coop/press/NewsReleases/Documents/InteroperabilityCyberSecurityPlan.pdf http://www.nreca.coop/press/NewsReleases/Documents/NRECAsecurityslides_release.pdf

Acronyms [1of3]

Abbreviation	Description
ADE	Automated Data Exchange
ADR	Automated Demand Response
AMI	Advanced Metering Infrastructure
ANSI:	American National Standards Institute
ARRA	American Reinvestment and Recovery Act
ASAP-SG	Advanced Security Acceleration Project for the Smart Grid
CERT	Computer Emergency Response Team
CIA	Confidentiality, Integrity, Availability
CIM	Common Information Model
CIP	Critical Infrastructure Protection
COS	SGIP Catalog of Standards
CSWG	Cyber security Working Group
DHS	Department of Homeland Se
DOD	Department of Defense
DOE	Department of Energy
DOE-OE	Department of Energy Office of Electric Delivery and Energy Reliability

Acronyms [2of3]

Abbreviation	Description
EEI	Edison Electric Institute
EPRI:	Electric Power Research Institute
ESPI	Energy service provider interface
FERC	Federal Energy Regulatory Commission
FFRDC	Federally Funded Research and Development Center
GWAC	GridWise Architecture Council
HAN	Home Area Network
ICCP	Inter-Control Center Communications Protocol
ICS	Industrial Control System
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineer
ISA	International Society of Automation
ISO	International Organization for Standardization
IT	Information Technology
KwH:	Kilowatt-Hour
MADRI	Mid-Atlantic Distributed Resources Initiative
NAESB	North American Energy Standards Board

Acronyms [3of3]

Abbreviation	Description
NARUC	National Association of Regulatory Utility Commissioners
NEMA	National Electrical Manufacturers Association
NERC	North American Electric Reliability Corporation
NESCO	National Electric Sector Cyber security Organization
NESCOR	National Electric Sector Cyber security Organization Resource
NIST	National Institute of Standards and Technology
NRECA	National Rural Electric Cooperative Association
OpenSG	Open Smart Grid is a technical subcommittee of the UCAIug Protection and Control
SCADA	Supervisory Control And Data Acquisition

Glossary [1of6]

Term	Description
Access Control	exerting control over who can interact with a resource
Alert	Notification that a specific attack has been directed at the information system of an organization
Assessment	the action of assessing or appraising
Asymmetric encryption	Public-key cryptography refers to a cryptographic system requiring two separate keys, one to lock or encrypt the plaintext, and one to unlock or decrypt the cypertext
Attack	any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an ass
Audit	evaluation of a person, organization, system, process, enterprise, project or product
Authenticate	To verify the identity of a user, user device, or other entity, or the integrity of data stored, transmitted, or otherwise exposed to unauthorized modification in an information system, or to establish the validity of a transmission
Authenticity	Refers to the veracity of the claim of origin or authorship of the information, non-repudiation

Glossary [2of6]

Term	Description
Authorization	the function of specifying access rights to resources, which is related to information security and computer security in general and to access control in particular
Availability	Having timely access to information
Back Door	In a computer system (or cryptosystem or algorithm) is a method of bypassing normal authentication, securing remote access to a computer, obtaining access to plaintext, and so on, while attempting to remain undetected
Compliance	Adherence to standards, regulations, and other requirements
Confidentiality	Refers to limits on who can get what kind of information
Countermeasures	Action, device, procedure, technique or other measure that reduces the vulnerability of an information system
Cryptography	practice and study of techniques for secure communication in the presence of third party
Cyber security	a branch of computer technology known as Information Security as applied to computers and networks. The objective of computer security includes protection of information and property from theft, corruption, or natural disaster, while allowing the information and property to remain accessible and productive to its intended users

Glossary [3of6]

Term	Description
Decryption	the reverse process of encryption
Defense-in-depth	practical strategy for achieving Information Assurance in today's highly networked environments. It is a "best practices" strategy in that it relies on the intelligent application of techniques and technologies that exist today. The strategy recommends a balance between the protection capability and cost, performance, and operational considerations.
Denial of Service	to make a computer resource unavailable to its intended users
Encryption	transforming information (referred to as plaintext) using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key
Firewall	A device or set of devices designed to permit or deny network transmissions based upon a set of rules and is frequently used to protect networks from unauthorized access while permitting legitimate communications to pass
Flooding	A simple routing algorithm in which every incoming packet is sent through every outgoing link

Glossary [4of6]

Term	Description
Governance	to consistent management, cohesive policies, guidance, processes and decision-rights for a given area of responsibility or an asset
Hacker	someone who accesses a computer system by circumventing its security system
Hazard	A situation that poses a level of threat to life, health, property, or environment
Integrity	being correct or consistent with the intended state of information. Any unauthorized modification of data, whether deliberate or accidental, is a breach of data integrity
Intrusion	Attempt to compromise the confidentiality, integrity or availability of a resource
Malicious Code	Software capable of performing an unauthorized process on an information system
Monitoring	Observe a situation for any changes which may occur over time
Packet	A formatted unit of data carried by a packet mode computer network
Pharming	hacker's attack aiming to redirect a website's traffic to another, bogus web site

Glossary [5of6]

Term	Description
Phishing	attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication
Risk Assessment	Determining the quantitative or qualitative value of risk related to a concrete situation and a recognized threat (also called hazard)
Risk	The potential that a chosen action or activity (including the choice of inaction) will lead to a loss (an undesirable outcome
Smurfing	A way of generating significant computer network traffic on a victim network. This is a type of denial-of-service attack that floods a target system via spoofed broadcast ping messages.
Spam	use of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately
Spoofing:	Falsifying data on a telecommunications network
Spyware	Software that collects information about a person or organization without their knowledge or informed consent and reports such data back to a third party

Glossary [6of6]

Term	Description
Symmetric encryption	Symmetric-key algorithms are a class of algorithms for cryptography that use trivially related, often identical, cryptographic keys for both encryption of plaintext and decryption of cipher text
Threat	Any circumstance or event with the potential to adversely impact an information system through unauthorized access, destruction, disclosure, modification of data, and/or denial of service
Virus	A computer program that can replicate itself and spread from one computer to another. The term "virus" is also commonly but erroneously used to refer to other types of malware, including but not limited to adware and spyware programs that do not have the reproductive ability
Vulnerability Assessment	The process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system
Vulnerability	The intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw
Whaling	A phishing scam that targets big game
Worm	self-replicating malware computer program, which uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention

Contact Information

Chuck Goldman
Lawrence Berkeley National Laboratory
CAGoldman@lbl.gov
510 486-4637

Sandy Backi
EnerNex Corporation
sandy.bacik@enernex.com
865-696-4470

Roger Levy
Smart Grid Technical Advisory Project
RogerL47@aol.com
916 487-0227